How to Survive DIACAP and Networthiness

August 21, 2008

Steve Briggs
Facility Dynamics Engineering

DIACAP is

- "identify and provide information security protections commensurate with risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems"

  -- From FISMA
- Replaces DITSCAP
- Required of ***any*** Army (DOD) Information System

3

Networthiness is

- Required of any Army "software application" that lives on the DOIM/basewide LAN
- Very similar requirements to DIACAP
- Less actual testing/validation that DIACAP
- Networthiness is more focused on protecting the network from the application
  - What network ports, what bandwidth, etc.
  - DIACAP is "strictly" IA

4

IACAPDay isnay anay holeway ewnay anguagelay

- ACA – Agents of the Certification Authority
  - People who actually perform validation. Think "Commissioning agent". Mostly reimbursable or contractors.
- AGM – Army Gold Master (Software)
  - A standard Army Windows-based OS
- APC – Area Processing Center
  - Army is consolidating it's servers off-post
- ATO/IATO/IATT – Authority To Operate, Interim ATO, Interim Authority To Test
  - Possible decisions (outcome) of DIACAP

5

- BBP – Best Business Practices
  - Many DIACAP policies/procedures use this
- CA – Certification Authority
  - Makes recommendation on IA. Think "Commissioning Authority"
- CCB – Configuration Control Board
  - Configuration Management of the UMCS
- CIO – Chief Information Officer/Office
- CON – Certificate of Networthiness
- CorpsLon – LNS-based LonWork installed in accordance with UFGS 23 09 23 and 25 10 10
- DAA – Designated Approving Authority
  - Responsible for DIACAP decision
- DIACAP – DOD Information Assurance Certification and Accreditation Process

6

- Enclave – a isolated/protected portion of the network
- IA – Information Assurance
- IAM – Information Assurance Manager
- IASO – Information Assurance Security Officer
  - Person responsible for IA for the system
- IPPID – IP Platform Interconnect Device
  - What DOIM/IA people will call the BPOC
- MAC – Mission Assurance Criticality
  - How important is system to the **warfighter**?
- MOU / MOA – Memorandum of Understanding/Agreement
  - Written agreement between DPW and DOIM for support of UMCS

7

- OIA&C – Office of Information Assurance and Compliance
- OS – (computer) Operating System: WinXX
- SIP – System Identification Profile (DIP)
  - Document that describes the system; starting point for DIACAP
- SLA – Service Level Agreement (with DOIM)
  - Service above/beyond common level of service
  - Synonymous with MOA/MOU
- "System" – What Networthiness calls an application that includes the Operating System

8

- STIG – Security Technical Implementation Guidelines
  - OS-specific guidance on how to secure the OS; for example, there's a specific STIG for WinXP
- POA&M – Plan of Activities and Milestones
  - A "get well" plan for a system that doesn't get an ATO from DIACAP
- VLAN – Virtual Local Area Network
  - IT to break one big LAN into several small ones
- VPN – Virtual Private Network
  - IT to run a secure network over an insecure (e.g. Internet) network
- 802.1x – An IT standard for securing network connections

References:

- Army Information Assurance Certification and Accreditation (C&A) Terms for Connectivity to the Installation Service Provider/ICAN Version 0.1 Draft
- Interim DOD C&A Process Guidance, July 2006
- DOD Instruction 8500.2 IA Implementation

9

DIACAP Drivers

- Federal Information Security Management Act of 2002 (FISMA)
- DoD Directive 8500.1 Information Assurance - applies to
  - "all DOD-owned or –controlled information systems that receive, process, store, display, or transmit DOD information."
  - "Stand-alone information systems"
  - Doesn't limit to basewide LAN systems
    - Includes RF, commercial broadband, etc.
  - Doesn't care if it's outsourced

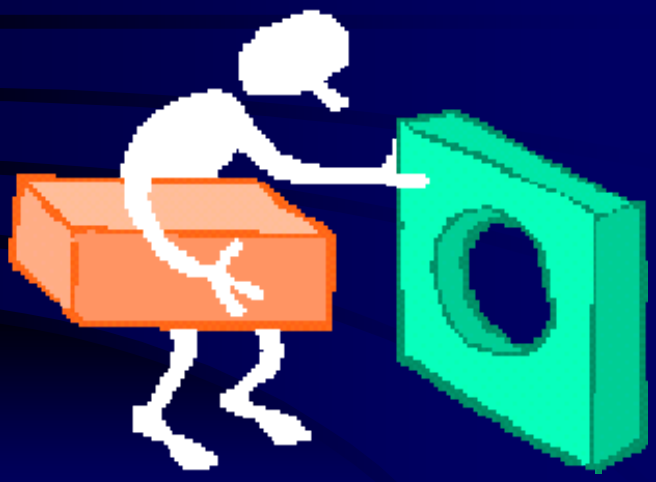
10

DIACAP was NOT designed with a UMCS in mind

- Centrally funded systems (CEFMS, etc)
  - UMCS are not centrally funded
- Centrally developed, sole source systems
  - UMCS is ***not*** sole source
  - Every one is slightly different
- Systems usually have a program manager
  - Our PM is harder to identify
- Systems are often static – they just deploy it.
  - UMCS constantly grows

11

Overview of UMCS DIACAP Process



12

How to meet DIACAP

- Best Answer:

–Don't Try

- Beg, Browbeat, Blackmail DOIM and use their DIACAP
- DOIM has (should have, must have?) a DIACAP approval for the basewide LAN

–Use it!

- For most installations/DOIMs, this seems to work
- Will need to document BAS for DOIM

13

How to NOT meet DIACAP
(get DOIM to meet it for you)

- BAS description; may use SIP from DIACAP
- Network architecture
  - Probably some sort of IP riser diagram and sample building Lon networks
- MOU/MOA/SLA
  - Clearly define DOIM responsibilities
- Certificate(s) of Networthiness for UMCS
- Risk assessment
  - What vulnerabilities are introduced by UMCS?
- This is by far the "path of least resistance"!

14

How to meet DIACAP

- Mostly IP / IT architecture requirements
- M&C server configuration requirements
- Lots of processes/procedures/people issues
- Not really covered under specs/UFCs
  - But, will probably add requirements to 25 10 10
- Big part falls on DOIM
  - Make them your ally, not your enemy!

15

Every system is different

- No global solution
  - Met with NETCOM to discuss “type” certification and “local” implementation
  - NETCOM said “no”, there’s no “generic” system to test; it’s just a document/concept
- Each UMCS needs its own DIACAP
- We (ERDC) will attempt to provide guidance
  - This will introduce additional constraints/requirements at the UMCS level

16

Template/Guidance

- Division of responsibilities between DPW and DOIM
- How to set up IP architecture/network
- How to set up M&C server
- How to set up M&C clients
- How to meet IA controls
- DIACAP roadmaps
- Template/sample DIACAP forms
- Q&A, some direct support ???

17

Ft Sill is the Bleeding Edge

- Furthest along (as far as we know)
- Only installation doing DIACAP……
- Greatest delay in UMCS contract (AFAIK)
- Many hurdles (past, present, future) in DPW, DOIM
- We are using Ft. Sill as our test case
- Trying to develop “generic” lessons learned

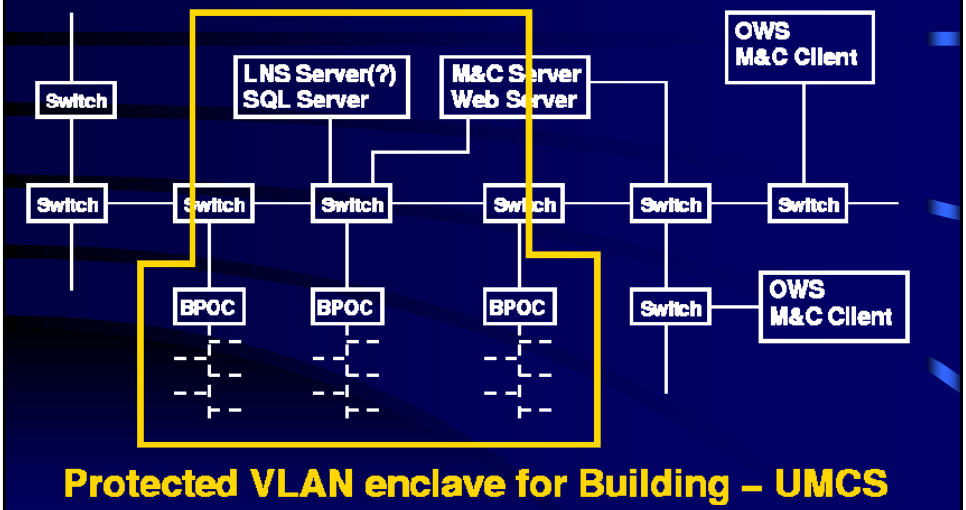
18

System IP / IT Architecture

- Get DOIM cooperation and support
  - IT security is ***their*** job, not yours!
  - Service Level Agreement, MOU, whatever
- Use Basewide LAN / IP network
  - VLAN "enclave" to buildings
  - VPN to M&C clients / OWSes
- DOIM is responsible for network security
- DOIM is responsible for PC OS security
- DPW is responsible for application security

19

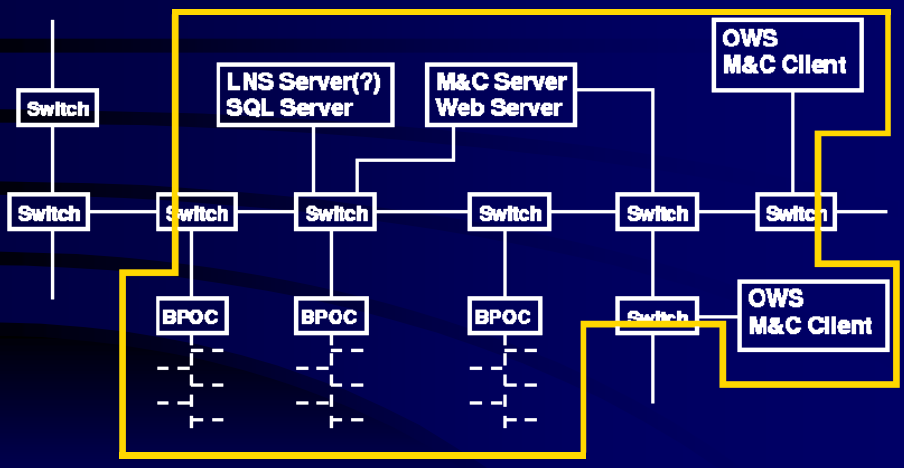
System IP / IT Architecture



Protected VLAN enclave for Building – UMCS

20

System IP / IT Architecture



Protected VLAN enclave for entire BAS

21

M&C Clients (OWSes)

- M&C server is isolated from all but BPOCs in buildings (exception: VPN connection to OWS)
  - May have limited number of fixed OWSes with access
- Must run VPN client on OWS to get to M&C server
- Must be on basewide LAN
  - No "remote" (off-base) access
  - Unless DOIM supports off-base VPN access, then the machine may appear to be on base as far as we know
    - May still be conflicts between 2 VPN clients

22

Why DOIM Involvement?

- They will want to administer the OS on any PC
  - Make it their responsibility
- They will want to administer any network you install
  - Make it their responsibility
- There's a lot of IA controls you don't want to deal with
  - "Going it alone" is possible, but ***ugly***!
  - Greatly increases your documentation/testing/verification burden
- It's ***their job, not yours!***

23

DIACAP Process

- System Identification Profile
- Determine needed IA controls
- Implement them
- Test implementation
- Develop "Get Well Plan"
  - if needed
- Get everything signed off on
- Get ATO

24

System Identification Profile (SIP)

- Will probably be needed even if you don't do DIACAP yourself!
- Registers UMCS with the DIACAP gods
  - "Hey, I've got a system here that needs DIACAP!"
- System name, owner, description
- Lots of questions I can't answer
- DPW and DOIM can answer them
- We'll get example UMCS SIPs as they become available

25

DIACAP Team

- System Owner – Probably DPW
  - But could be the Garrison Commander
- DAA – Not sure. Probably someone at IMCOM or NETCOM (?) or CIO/G6 (?)
  - Can't be the System Owner
  - Must be a G.O. or SES
- CA – CIO/G-6
- ACA – ISEC is accredited ACA
  - List of ACAs on OI&C website
  - CE-LCMC SEC -- S&TDC -- ARL CISD
  - ARL/SLAD -- SPAWARSYCEN Charleston
- IASO – DOIM, maybe DPW staff as well

26

System Classification

- How Critical is this system to the warfighter?
  - MAC I A Lot!
  - MAC II A Little.
  - MAC III Not.
    - ***We are MAC III***
- How sensitive is the information?
  - Classified
  - Sensitive
    - This is the default for anything on the DOIM LAN
    - ***We are sensitive***… but may not have any sensitive information in the system
  - Public

27

Information Assurance (IA) Controls

- For each Classification (MAC & sensitivity level), there is a set of IA controls
- The higher the level, the more controls (and the harder they become)
  - MAC III Public has 75 controls
  - ***MAC III Sensitive has 100 controls (and many of the 75 "carry over" are harder)***
- To get ATO, "must" meet all controls
  - Can get IATO with a POA&M (get well plan)

28

Sensitive vs. Public

- May want to purposely exclude truly sensitive information
- We're the 90% solution; we do a lot of barracks, Admin, dining halls, Battalion HQs
- Some "sensitive" controls may not make sense:
  - A control says monitors must be positioned so they can't be viewed by "unauthorized" viewers
    - Who is "authorized"?
    - Is everyone (excluding visitors) "authorized"?
    - Is this really applied to every machine on base?
- It's OK if some controls are just "N/A"

29

How to handle critical facilities?

- Picture a data center with packaged Liebert DX units needing only electricity
- Allowing remote shutdown or "excessive" setpoint adjustment creates HUGE vulnerabilities
- How do you connect this to the UMCS?
- Answer: Program Liebert to limit functionality from UMCS:
  - Data center runs 24/7 – Don't need/allow remote shutdown – make sure points schedule shows this!
  - Data center is "always" 68 F – Don't need/allow remote setpoint adjustments

30

IA Controls

- Do not focus on Lon devices
  - They're not IP
  - Do need to discuss because they have a network
  - Emphasize they do control, not IT
  - ***IF*** they have security, need to use it
- May configure BPOC so it's dumb
  - No remote configuration or access
  - Make it just a dumb Lon to IP router
  - Don't use Configuration Server
    - unsure about DHCP
- Network – DOIM's problem
- M&C Server – big problem, lots of work
- Clients – non-web based may be a problem

31

IA Controls Subject Areas

- Continuity: Backups, Alternate site, reliability, disaster recovery
- Security Design and Configuration: General system design, processes, procedures
- Enclave Boundary Defense: Securing the connection between the UMCS and "outside"
- Enclave Computing Environment: Audit trails, access control, need-to-know, least privilege, "other" connections

32

- Identification and Authentication: Accounts, Passwords
- Physical and Environmental: Physical security, lighting, fire, environmental (HVAC!), power
- Personnel: Proper screening for UMCS users, UMCS administrators, PC administrators
- Vulnerability and Incident Management: Planning and procedures for incidents and vulnerabilities

33

ACA / Security Engineer

- May want to get "expert" help above and beyond DOIM
  - DOIM may not have sufficient IA expertise
  - DOIM probably doesn't understand UMCS
- Need to write a good SLA with DOIM
  - We will probably "publish" samples/guidance
- Might be DOIM's responsibility, but it's ***your*** problem if you don't meet the controls
- Plan for multiple visits from the ACA
- Get them involved early
- Analogy to Commissioning process

34

At least 3 visits from ACA

- 1: Planning
  - Discuss system and how you will meet IA controls
  - Think “Cx kick-off meeting during design phase”
- 2: Pre-test visit
  - Where are you, what are implementation problems and how will you deal with them
  - Think “review of contractor start-up testing”
- 3: Testing
  - Actual validation of controls
  - Think “Cx agent does their tests”
- 4+ Up: Repeat and try and get it right

35

IA Control Validation

- For each IA control, there are validation procedures
- ACAs perform validation
- Many of the controls are policy/procedural
- Many of the validation procedures are of the form “review XXX documentation”
- Quite possible to “pre-verify” some controls prior to actual system startup
  - Could do during 2nd ACA visit
  - Reduce uncertainty of waiting until the very end

36

DIACAP Scorecard, POA&M

- ACAs validate controls
- ACAs prepare DIACAP Scorecard, which rates the UMCS vs. each IA control
- For controls that aren't met, statements of weakness are developed (how it failed)
- From these, a Plan of Action & Milestones is developed
  - This details how to correct each weakness

37

DIACAP Decision

- Scorecard, and POA&M (if needed) get compiled into Comprehensive DIACAP Package
- Forwarded to CIO/G6 for review and recommendation
- DAA makes decision
  - ATO: No POA&M, you're done.
    - Review every year
    - Re-apply every 3 years
  - IATO: Execute POA&M and try again

38

Networthiness

- Similar to DIACAP
- Need CON to get software installed by DOIM
- Need DIACAP "decision" to get CON
- May not be able to validate system as part of DIACAP unless system is up and running (perhaps isolated from everything, but at least the PC is running)
- There is no CON for hardware….
  - Not clear what the approval process – or if it's needed
- There's a form to fill out and submit

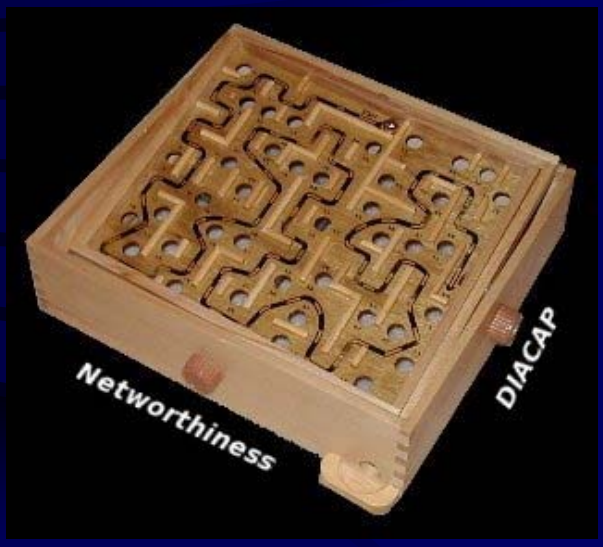
39

Networthiness Form

- System identification - name and owner
- Purpose - capabilities / replacing something?
- IT impact - bandwidth, transactions, protocols, ports, servers, web servers
- System design
- Security
- Documentation, manuals
- Classified data?

40

Networthiness and DIACAP



But… put on a blindfold first

41

A New Hope

- IF you're under DOIM's DIACAP, it's not an issue!
- Can get a DIACAP IATT ***before*** system is implemented
  - Not the "normal" decision people want
- Can use IATT to fill out Networthiness checklist
- Can get CON
- Can install software and proceed with "real" DIACAP goal

42

(DIACAP) Process

- DOIM / DPW fill out SIP and IATT checklist
- IATT is for a period of time
  - Ask for at least 90 days!
  - Realistically, ask for 120 – 180 days
    - Don't want to get caught waiting on DIACAP approval
- ACA reviews it
- CIO/G6 blesses it
- Get DIACAP IATT decision
- Submit for CON
- Get CON
- Continue with DIACAP IA testing

43

All this is slow

- ACAs are booked solid for months
- CIO/G6 is taking 2 – 3 months for approvals
- Need to get things moving on as many fronts as possible ASAP
  - Start budgeting money
  - Start looking for ACAs
  - Start getting agreements with DOIM
  - Start getting procedures/policies in place
  - Start SIP / Networthiness checklist
    - ***Get in the DIACAP queue!***

44

DIACAP Costs

- Budget for at least $50k (more?) for the ACA and/or Security Engineer
- ***IF*** you wanna do it on the cheap:
  - At least $15k and a couple weeks on site for ACA validation
  - ***Assuming*** everything goes smoothly
  - Assuming no repeat visits
    - One repeat visit because you didn't pass the first time will kill your budget and timeline
- Can you afford the risk of doing it "cheap"?
- Additional DOIM costs for SLA?

45

Are computers GFE?

- OS must be STIG compliant and based on AGM
- How does this happen?
- Can vendor deliver pre-installed AGM?
- Does DOIM provide a machine with a STIG-compliant OS to the vendor?

46

Local Admin Rights

- Who does updates for application software?
  - M&C Software, LNS plug-ins, etc.
- May want DPW staff with local admin rights
- May be easy:
  - Request from DPW to DOIM
    - DOIM must track users with admin rights
  - Short (1 day?) online IA training & certificate
- Other DOIMs may have more onerous requirements
  - We may be able to help out there

47

Software Updates

- ***All*** must go through CCB
- Will depend on IA impact of software
  - LNS plug-ins will be minor
  - M&C software – depends: Does it have IA components?
  - May be STIGs on applications – ask ACAs for help
- Things with major IA impact are ***painful***
  - Windows, IIS (Web Server), MS-SQL (database)
  - Do risk assessment, DIACAP package, re-submit
  - Hopefully, not ***too*** painful, but will need ACA involvement
- Most things with IA impact are DOIM responsibility
- Use CCB to block unnecessary painful changes
  - As system owner, you have a say in the CCB

48

eMASS
Enterprise Mission Assurance Support Service

- Currently, DIACAP is largely a paper process
- eMASS is supposed to automate tracking/documentation
  - Manage key DIACAP activities
  - Facilitate system registration
  - Assign baseline IA controls
  - Generates Certification and Accreditation flowchart
  - Facilitate processing of Federal reporting requirements
  - Generate reports
  - Track status
- Don't know how useful it may be
  - No one has said "Yes, use it"

49

Conclusions:

- DIACAP:
  - replaces DITSCAP
  - required for all Army information systems
  - PAINFUL
- Best bet is to be covered under existing DOIM DIACAP
  - (refer back to "How to NOT meet DIACAP" – slide #14)
- Networthiness:
  - needed for any software on the LAN – M&C software, LNS tools, programming software, etc.
  - Fill out a form, submit it, and wait – not too painful
  - Check your software – it may already be covered
- **Work with DOIM**

50

Other resources

- https://diacap.iaportal.navy.mil
  - Main DIACAP portal
- https://www.us.army.mil/suite/portal/index.jsp
  - Main Army IA page
- http://www.army.mil/ciog6/networthiness.html
  - Main Networthiness page (not very helpful…)
- US Army Information Systems Engineering Command
  - Ms Jackie Tregre
  - (520) 538-6665
  - tregrej@hqisec.army.mil
    - Fred Abbitt @ ISEC has spoken with Steve Briggs and Joe Bush

51

Questions?

- Joe Bush
  - Joseph.Bush3@us.army.mil
  - 217-352-6511 (ERDC/CERL main number)
- Steve Briggs
  - zzybaloobah@yahoo.com
  - 217-356-3218

52